

How much is a quantum controller controlled by the controlled system?

Dominik Janzing* and Thomas Decker†

August 20, 2007

Abstract

We consider unitary transformations on a bipartite system $A \times B$. To what extent entails the ability to transmit information from A to B the ability to transfer information in the converse direction? We prove a dimension-dependent lower bound on the classical channel capacity $C(A \leftarrow B)$ in terms of the capacity $C(A \rightarrow B)$ for the case that the bipartite unitary operation consists of controlled local unitaries on B conditioned on basis states on A . This can be interpreted as a statement on the strength of the inevitable backaction of a quantum system on its controller.

If the local operations are given by the regular representation of a finite group G we have $C(A \rightarrow B) = \log |G|$ and $C(A \leftarrow B) = \log N$ where N is the sum over the degrees of all inequivalent representations. Hence the information deficit $C(A \rightarrow B) - C(A \leftarrow B)$ between the forward and the backward capacity depends on the “non-abelianness” of the control group. For regular representations, the ratio between backward and forward capacities cannot be smaller than $1/2$. The symmetric group S_n reaches this bound asymptotically. However, for the general case (without group structure) all bounds must depend on the dimensions since it is known that the ratio can tend to zero.

1 Introduction and formal setting

The fact that no measurement can extract information about a quantum system without disturbing its state is one of the essential features of quantum theory [1, 2]. Roughly speaking, it is therefore true that the measurement apparatus influences always the quantum system when the system influences the measurement apparatus. For this reason, bidirectionality of causal influences seems to be a general feature of quantum theory. However, measurement-disturbance relations [3] for quantum measurements

*School of Computer Science and Electrical Engineering, University of Central Florida, Orlando, FL 32816, USA. Electronic address: janzing@ira.uka.de

†Department of Computer Science & Engineering, University of Washington, Seattle, WA 98195, USA. Electronic address: decker@ira.uka.de

do not provide a general answer to the following question: to what extent is the state of the measured system influenced by the *state* of the measurement apparatus? This question refers to a stronger sense of causal bidirectionality: Whenever an interaction between two systems A and B allows us to transmit information from A to B then it also enables information transfer from B to A . In this article we show that (1) such a stronger sense of causal bidirectionality is true for interactions between *finite* dimensional quantum systems but violated in infinite dimensions and (2) there is a dimension-dependent lower bound on the channel capacity from B to A in terms of the capacity from A to B .

The motivating example to study quantitative relations between the information that can be transmitted from A to B and the amount of information that can be sent in the converse direction is the well-known symmetry of the controlled-not gate (“CNOT”) [4]. Let U be a CNOT gate with qubit A as *control* wire and qubit B as *target* wire. This gate allows us to transmit the classical information 1 bit from A to B : To this end, we initialize B to the basis state $|0\rangle$ and choose one of the states $|0\rangle, |1\rangle$ for system A . After applying CNOT to the joint system the state of B will be $|0\rangle$ or $|1\rangle$ depending on which state we have chosen for A . Since the roles of control wire and target wire are swapped when the CNOT gate is described in the Hadamard basis we can also transmit 1 classical bit of information from B to A after we have initialized A to the state $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$. A possible generalization of this symmetry is the following observation. Let $P_j := |j\rangle\langle j|$ for $j = 0, \dots, n-1$ be the projector onto the span of the j th canonical basis vector in \mathbb{C}^n and S be the cyclic shift operator on \mathbb{C}^n defined by

$$S := \sum_{j=0}^{n-1} |j\rangle\langle (j+1) \bmod n|.$$

Then we introduce controlled powers of the shift by

$$U := \sum_{j=0}^{n-1} P_j \otimes S^j. \quad (1)$$

Elementary algebra shows that a conjugation of U with a Fourier transform [4] on both components leads to

$$\tilde{U} := \sum_{j=0}^{n-1} S^{-j} \otimes P_j.$$

Since U allows us to send the information $\log_2 n$ bits from A to B we can also transfer $\log_2 n$ bits in the converse direction by initializing A in one of the Fourier transformed basis states. Because this symmetry does not apply to general unitary transformations U we want to understand how to quantify the amount of information that can be transferred backwards in the general case.

The motivation to ask this type of questions is given by the following background:

- **Understanding causality.** The statement that two physical systems *interact* defines, in the first place, a symmetric relation. On the other hand, it is a matter of fact that there are situations where the effect of one physical system on a second

one is more relevant than the effect of the latter on the former. To understand under what conditions causal unidirectionality emerges in a way that is consistent with Hilbert space quantum mechanics would be another small step towards a deeper understanding of the physics of causal directions.

- **Understanding fundamental limits of quantum control.** A quantum controller is a device that influences a quantum system in a desired and flexible way. Quantum control is often phrased in terms of time-dependent Hamiltonians [5, 6], taken from one parameterized set of Hamiltonians. This description refers to the controller as a classical system. Even though this perspective is very helpful for practical purposes, the following fundamental point of view may be more helpful to understand the limits and the thermodynamics of quantum control: actually, the interaction between controller and system induces a joint dynamics of the bipartite quantum system (which may, in addition, also involve the environment as a third system). Surprisingly, this perspective has rarely [7, 8] been discussed in the context of quantum control even though it was quite popular in the context of quantum measurements [9]. As noted in [7] the arbitrariness of the so-called “Heisenberg cut” between the system to be measured and the measurement apparatus occurs also in the quantum control setting: The question “who controls the quantum controller?” could lead to a never ending sequence of “meta-controllers” and consistency of quantum theory requires that we can shift the cut between the controlled system and its controller. Toy models for a consistent shift of this kind have been described in [7]. When asking which feature makes a quantum system interacting with another system the controller of the latter, it is natural to explore to what extent the controller is immune to changes of the state of the former. We do not claim that this immunity is a necessary or sufficient feature of a quantum controller. Nevertheless, we are convinced that the thermodynamic limits of quantum control are related to the question which amount of information is transferred to the controller.
- **Generalizations of the phase kick-back.** The symmetry of CNOT, or, more general, the symmetry of the controlled powers of the cyclic shift is just an instance of the well-known phase kick-back that is used in quantum phase estimation [10]. It has been shown that every quantum algorithm can be rewritten in such a way that it contains phase estimation as its central part [11]. For this reason, it is desirable to understand in which sense there are generalizations of the phase kick-back to non-abelian groups. The group structure is actually of minor relevance for the above philosophy-focused questions. However, representation theory of finite groups will provide us with nice examples where the backaction can be analyzed.
- **Limits of classical concepts of low power computing.** Due to progressing miniaturization quantum effects are expected to play a dominant role in future computing devices. A characteristic feature of current technology is the well-defined direction of the information flow: The input of a device is supposed to control the output, not vice versa. Likewise, the clock signal is supposed to trigger logical operations and not the other way round. To what extent an unidirectionality of this kind is possible if the complete dynamics of the computation process

is dominated by quantum uncertainties is an open question. Limits of this kind have, for instance, been discussed in [12, 13, 14, 15].

To address the above questions we describe the quantum systems A and B by Hilbert spaces \mathcal{H}_A and \mathcal{H}_B , respectively, and consider a unitary operation U on $\mathcal{H}_A \otimes \mathcal{H}_B$. Assume both systems are independently initialized into quantum states ρ_A and ρ_B . For every state ρ_B we obtain a channel

$$G_{(A \rightarrow B)}(\rho_A) := \text{tr}_B(U(\rho_A \otimes \rho_B)U^\dagger)$$

and a ρ_A -dependent “backwards” channel

$$G_{(A \leftarrow B)}(\rho_B) := \text{tr}_A(U(\rho_A \otimes \rho_B)U^\dagger).$$

Note that we have dropped the dependence of ρ_B and ρ_A , respectively, in our notation. We define the forward channel capacity by the maximal amount of Holevo information [4] that can be sent from A to B :

$$C(A \rightarrow B) := \sup \left\{ S \left(G_{A \rightarrow B} \left(\sum_j p_j \gamma_j \right) \right) - \sum_j p_j S \left(G_{A \rightarrow B}(\gamma_j) \right) \right\},$$

where the supremum is taken over all ensembles $\{p_j, \gamma_j\}$ of density operators acting on \mathcal{H}_A and all possible initializations ρ_B . Here S denotes the von-Neumann entropy. This capacity has been called Holevo-Schumacher-Westmoreland capacity in [16]. It has been shown to be the maximal amount of classical information that can be sent when multiple copies of the channel are available and the receiver is able to perform arbitrary joint measurements on the joint output state [17]. The motivation to focus on the *classical* information capacity rather than on the *quantum* capacity is that the ability to transfer classical information is already a clear indication for B *influencing* A . The backward capacity is defined in an analogous way. In terms of these definitions, the goal of this paper is to understand under which circumstances $C(A \leftarrow B)$ can be small even though $C(A \rightarrow B)$ is large. Bipartite unitary gates as communication resources have, for instance, been studied in [18, 19]. The major part of the literature that appeared in this context focuses on the capabilities of creating entanglement [20, 21, 22, 23, 24, 25, 26, 27, 28], but studies also the relation to classical information capacities [29] for the special case of two-qubit systems. However, a profound understanding of these relations and tight bounds on backward capacities in terms of forward capacities in arbitrary dimensions are still missing.

2 Qualitative statements

We have emphasized that the questions of this article are not answered by the known information-disturbance relations in any obvious sense. The following observation makes this difference more apparent: if an interaction transmits information about an unknown quantum state of A to B then it changes necessarily the state of A . This holds regardless of the Hilbert space dimensions of A and B . However, in infinite dimensions, the way how the interaction changes the state of A can be completely independent of

the state of B . In other words, in infinite dimensions we may have forward information transmission without backward information transmission even though measurement-disturbance relations remain valid:

Lemma 1 *There exists unitary operations acting on two quantum systems with separable infinite dimensional Hilbert spaces such that $C(A \rightarrow B) \neq 0$ but $C(A \leftarrow B) = 0$.*

Proof: Let \mathcal{H}_A and \mathcal{H}_B be spanned by basis vectors labeled by the binary sequences

$$(a_n)_{n=0,-1,-2,-3,\dots} \quad \text{and} \quad (b_n)_{n=1,2,3,\dots} \quad \text{with} \quad a_n, b_n \in \{0, 1\}$$

respectively, each sequence $(a_n)_n$ and $(b_n)_n$ containing finitely many symbols 1. The tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ can be canonically identified with a space whose basis vectors are labeled by the binary sequences $(c_n)_{n \in \mathbb{Z}}$ having finite Hamming weight since \mathcal{H}_B corresponds to the positive numbers and \mathcal{H}_A to the negative numbers and 0. We can think of the system as an infinite chain of quantum bits (“qubits”) with the additional restriction that only a finite set of qubits are in its upper state. A right shift of basis vectors induced by the right shift on \mathbb{Z} is given by

$$(c_n)_{n \in \mathbb{Z}} \mapsto (c_{n-1})_{n \in \mathbb{Z}},$$

and will clearly allow us to send one bit from A to B because the state of the rightmost qubit of A is shifted to B . Nevertheless, the state of A is completely immune with respect to changing the state of B before the shift has been applied because the final state of A is simply given by shifting the state of the chain that corresponds to the values $n \leq -1$ one site to the right. \square

However, in finite dimensions we have [18]:

Theorem 1 *Let \mathcal{H}_A be finite dimensional. If for some unitary U on $\mathcal{H}_A \otimes \mathcal{H}_B$ the backward channel capacity satisfies $C(A \leftarrow B) = 0$ then also $C(A \rightarrow B) = 0$.*

We give an alternative proof that is purely algebraic and makes apparent that finite dimensionality is only needed for A :

Proof: Assume $C(A \leftarrow B) = 0$. Then there is no observable A on \mathcal{H}_A whose expected value changes if we apply a unitary transformation $\mathbf{1} \otimes V$ to a state $\rho_A \otimes \rho_B$. Hence we have

$$\text{tr}((\mathbf{1} \otimes V)U(A \otimes \mathbf{1})U^\dagger(\mathbf{1} \otimes V^\dagger)\rho_A \otimes \rho_B) = \text{tr}(U(A \otimes \mathbf{1})U^\dagger\rho_A \otimes \rho_B).$$

Since this statement holds for all ρ_A, ρ_B we conclude

$$(\mathbf{1} \otimes V)U(A \otimes \mathbf{1})U^\dagger(\mathbf{1} \otimes V^\dagger) = U(A \otimes \mathbf{1})U^\dagger$$

for all unitary operations V on \mathcal{H}_B . Hence $(\mathbf{1} \otimes V)$ commutes with all $U(A \otimes \mathbf{1})U^\dagger$ for all V, A . Let \mathcal{M}_A and \mathcal{M}_B be the algebra of operators on \mathcal{H}_A and \mathcal{H}_B , respectively. The commutant of the algebra $\mathbf{1} \otimes \mathcal{M}_B$ is given by $\mathcal{M}_A \otimes \mathbf{1}$. Hence $U(\mathcal{M}_A \otimes \mathbf{1})U^\dagger \subset \mathcal{M}_A \otimes \mathbf{1}$. For this reason, the conjugation with U defines an injective C^* -homomorphism (see e.g. [30]) $\mathcal{M}_A \otimes \mathbf{1} \rightarrow \mathcal{M}_A \otimes \mathbf{1}$. Since \mathcal{H}_A is finite dimensional it is also surjective

and hence a C^* -automorphism. For matrix algebras, every such automorphism is inner [30], i.e., given by conjugation with one of its unitary elements.

Hence there is some $W \in \mathcal{M}_A$ such that $U(A \otimes \mathbf{1})U^\dagger = WAW^\dagger \otimes \mathbf{1}$ for all $A \in \mathcal{M}_A$. This implies that $(W^\dagger \otimes \mathbf{1})U$ commutes with $\mathcal{M}_A \otimes \mathbf{1}$ and is therefore an element of $\mathbf{1} \otimes \mathcal{M}_B$. Hence U has the form $U = W \otimes Y$ for some unitary operators W, Y . This is certainly a symmetric statement with respect to swapping the systems A and B . \square

3 Generalizing the CNOT symmetry

It would be interesting to know the class of unitary transformations for which $C(A \leftarrow B) = C(A \rightarrow B)$. This equality is, for instance, true for every U acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$ because U can be decomposed [31] as

$$U = (W_A \otimes W_B) \exp \left(i \sum_{\alpha=x,y,z} c_\alpha \sigma_\alpha \otimes \sigma_\alpha \right) (V_A \otimes V_B) \quad \text{with} \quad c_\alpha \in \mathbb{R}. \quad (2)$$

Since the local unitaries W_A, W_B, V_A, V_B are irrelevant, U can be simplified to an operator that is symmetric in A and B . However, in view of the philosophical questions raised in the introduction, statements that refer to particular dimensions are only of minor interest. The following set of bipartite unitaries defines a significant generalization compared to the ones given by conjugating the operator U in Eq. (1) with local unitaries on both components:

Theorem 2 *Let U be a unitary on $\mathbb{C}^n \otimes \mathbb{C}^m$ of the form*

$$U = (V_A \otimes V_B) D (W_A \otimes W_B),$$

where D is diagonal in some product basis and V_A, V_B, W_A, W_B are local unitaries. Then $C(A \rightarrow B) = C(A \leftarrow B)$.

Proof: Assume

$$U = D = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} d_{ij} |i\rangle \otimes |j\rangle$$

without loss of generality. It is clear that the optimal amount of information transfer can be achieved with pure states. It is furthermore obvious that the optimum from A to B can be achieved using basis states on A . This is because superpositions of basis states lead to mixtures of the corresponding output states on B . Assume we choose basis state $|i\rangle$ with probability p_i and we have B initialized to the state

$$|\psi\rangle = \sum_{j=0}^{m-1} c_j |j\rangle.$$

Given that the state $|i\rangle$ has been chosen for A we obtain for B the pure state

$$|\phi_i\rangle := \sum_{j=0}^{m-1} d_{ij} c_j |j\rangle.$$

Since the output states are pure the Holevo information transferred to B is given by the von-Neumann entropy of the mixture of outputs, i.e., by

$$S(\gamma) \quad \text{with} \quad \gamma := \sum_{i=0}^{n-1} p_i |\phi_i\rangle\langle\phi_i|.$$

We introduce the matrix

$$\Phi := \left(|\phi_0\rangle, |\phi_1\rangle, \dots, |\phi_{n-1}\rangle \right),$$

and rewrite Φ as the product $\mathcal{C}\mathcal{D}$ where \mathcal{D} denotes the $n \times m$ matrix with entries d_{ji} and \mathcal{C} is defined by

$$\mathcal{C} := \text{diag}(c_0, \dots, c_{m-1}).$$

Then we can write γ as

$$\gamma = \mathcal{C}\mathcal{D}\mathcal{Q}\mathcal{Q}^\dagger\mathcal{D}^\dagger\mathcal{C}^\dagger,$$

where

$$\mathcal{Q} := \text{diag}(\sqrt{p_0}, \dots, \sqrt{p_{n-1}}).$$

Since for any two matrices M the spectra of MM^\dagger and $M^\dagger M$ coincide the spectrum of γ coincides with the spectrum of

$$\mathcal{Q}^\dagger\mathcal{D}^\dagger\mathcal{C}^\dagger\mathcal{C}\mathcal{D}\mathcal{Q}.$$

This is exactly the density matrix we obtain if we choose the basis states $|j\rangle$ on B with probability $|c_j|^2$ and prepare A in the state

$$\sum_{i=0}^{n-1} \sqrt{p_i} |i\rangle.$$

This shows that for every protocol that sends basis states from A to B we can construct a scenario to transmit the same amount of information from B to A . \square

4 Lower bound on the backward capacity for controlled operations

In the remaining part of the paper we will restrict our attention to unitary operators that are unitaries on B controlled by basis states of A . Using the projections $P_j = |j\rangle\langle j|$ for $j = 0, \dots, n-1$ we define U on $\mathbb{C}^n \otimes \mathbb{C}^m$ by

$$U := \sum_{j=0}^{n-1} P_j \otimes V_j, \tag{3}$$

where each V_j acts on \mathbb{C}^m . If A is initialized to the state

$$|\phi\rangle = \sum_{j=0}^{n-1} c_j |j\rangle,$$

the input state $|\psi\rangle$ on B leads to the state

$$G_{A \leftarrow B}(|\psi\rangle\langle\psi|) = \sum_{i,j=0}^{n-1} \bar{c}_i c_j |i\rangle\langle j| \langle\psi| V_i^\dagger V_j |\psi\rangle. \quad (4)$$

We obtain a lower bound on $C(A \leftarrow B)$ in terms of a quantity that measures how much the operators V_j differ with respect to the operator norm:

Theorem 3 *Given a bipartite unitary operation of the form (3). Let*

$$d := \max_{j,k} \min_{\phi} \|V_j - V_k e^{i\phi}\| \quad (5)$$

be the maximal distance between the transformations V_j . Then

$$C(A \leftarrow B) \geq H_2\left(\frac{1}{2} + \frac{\sqrt{1-d^2/4}}{2}\right), \quad (6)$$

where $H_2(x) := -x \log_2(x) - (1-x) \log_2(1-x)$ denotes the binary entropy function.

Proof: Let A be initialized to the state

$$|\phi\rangle := \frac{1}{\sqrt{2}}(|j\rangle + |k\rangle),$$

where j, k denote the pair maximizing expression (5). Let $|\psi_1\rangle, |\psi_2\rangle$ be eigenstates of $U_j U_k^\dagger$ with eigenvalues $e^{i\mu_1}$ and $e^{i\mu_2}$ such that $|e^{i\mu_1} - e^{i\mu_2}| = d$. Then

$$\ell := \frac{1}{2}(e^{i\mu_1} + e^{i\mu_2})$$

has the absolute value $|\ell| = \sqrt{1-d^2/4}$. If one chooses one of the states $|\psi_p\rangle$ with $p = 1, 2$ it follows from Eq. (4) that the output state is given by a pure state. It is supported by the two-dimensional space spanned by $|j\rangle$ and $|k\rangle$ and reads:

$$\sigma_p := \frac{1}{2} \begin{pmatrix} 1 & e^{i\mu_p} \\ e^{-i\mu_p} & 1 \end{pmatrix}. \quad (7)$$

The uniform mixture

$$\frac{1}{2}(\sigma_1 + \sigma_2)$$

has the off-diagonal entries $\ell/2$ and $\bar{\ell}/2$ and thus the eigenvalues $1/2 \pm |\ell|/2$. Its entropy is therefore given by $H_2(1/2 + |\ell|/2)$. \square

Given the maximal distance d we can derive a dimension-dependent upper bound on the forward channel capacity:

Lemma 2 *Let V_j be a set of unitaries with a given maximal distance d . Then*

$$C(A \rightarrow B) \leq \min \left\{ \log k, H_2(d/2) + \frac{d}{2} \log(k-1) \right\},$$

where k is the minimum of n and m .

Proof: Let $|\psi\rangle$ be the state of B . If one chooses the j th basis state of A with probability p_j one obtains on B the state $V_j|\psi\rangle\langle\psi|V_j^\dagger$ with probability p_j . The entropy of the mixture

$$\sigma := \sum_j p_j V_j |\psi\rangle\langle\psi| V_j^\dagger$$

coincides with $C(A \rightarrow B)$ if the optimal pair p and $|\psi\rangle$ have been chosen. The entropy can be bounded from above as follows. Due to

$$\|V_j|\psi\rangle\langle\psi|V_j^\dagger - V_0|\psi\rangle\langle\psi|V_0^\dagger\|_1 \leq d$$

and the convexity of the trace norm we have

$$\|\sigma - V_0|\psi\rangle\langle\psi|V_0^\dagger\|_1 \leq d. \quad (8)$$

The rank of σ is at most $k := \min\{n, m\}$. Let q_1, \dots, q_k be the diagonal entries of σ with respect to a basis of the image of σ that contains $V_0|\psi\rangle$ as its first basis vector. We derive an upper bound on the probability distribution q which is also an upper bound on the von Neumann entropy of σ . The diagonal entries of $V_0|\psi\rangle\langle\psi|V_0^\dagger$ are $1, 0, \dots, 0$ and the trace-norm distance on the left hand side of Eq. (8) is at least $2 \sum_{j \geq 2} q_j$. This implies $s := \sum_{j \geq 2} q_j \leq d/2$. If $d/2 \geq (k-1)/k$ then q could even be the uniform distribution and we obtain only the trivial bound $S(\sigma) \leq \log k$. Otherwise, we obtain maximal Shannon entropy for q if we distribute s uniformly on the indices $2, \dots, k$ which is the distribution $1 - d/(2k-2), d/(2k-2), d/(2k-2), \dots, d/(2k-2)$. Its Shannon entropy is $H_2(d/2) + (d/2) \log(k-1)$. \square

The right hand side of Ineq. (2) is a strictly monotonic function $d \mapsto f(d)$ for $d \leq 2(k-1)/k$. In this regime we have therefore the bound

$$d \geq f^{-1}(C(A \rightarrow B)).$$

By inserting the right hand side into Ineq. (6) we obtain an explicit lower bound on $C(A \leftarrow B)$ in terms of $C(A \rightarrow B)$.

The ratio between backward and forward capacity allowed by this bound gets small for high dimensions. But this has to be the case because there is a gate [19] in dimension $n \times n$ for which the forward capacity is $\log n$ and the backward capacity is $O(\log \log n)$. The gate is of the form $U = P_j \otimes V_j$ with

$$\begin{aligned} V_j|0\rangle &= |j\rangle \\ V_j|i\rangle &= |i-1\rangle \text{ for } 0 < i \leq j, \quad \text{and} \quad V_j|i\rangle = |i\rangle \text{ for } i > j. \end{aligned}$$

Tight bounds on the ratio $C(A \leftarrow B)/C(A \rightarrow B)$ are, however, not known.

5 Regular representations of finite groups

Now we restrict our attention to the case where $U = \sum_j P_j \otimes V_j$ acts on systems with equal dimension n . The extreme case $C(A \rightarrow B) = \log n$ is of course of special interest. Then the V_j are sufficiently different to generate mutually orthogonal states from a

given one. The following construction provides a family of unitaries that satisfy this condition and have enough structure to allow us a systematic analysis. Even though this construction does not describe any real physical system, it is nevertheless helpful because the goal of this paper is to explore limitations on the relation between action and backaction that follow from Hilbert space geometry alone without any specific physical assumptions.

Let G be a group with $|G| = n$ elements and $(V_g)_{g \in G}$ be the permutation matrices corresponding to the regular representation of G . We label the basis states of \mathbb{C}^n by the elements $g \in G$ and denote them by $|g\rangle$. We define

$$U := \sum_{g \in G} P_g \otimes V_g. \quad (9)$$

By initializing B to the state $|\mathbf{1}\rangle$, where $\mathbf{1} \in G$ denotes the identity element, we clearly can obtain n mutually orthogonal states $|g\rangle$ in B by choosing the states $|g\rangle$ with $g \in G$ as inputs, i.e., $C(A \rightarrow B) = \log |G|$. Then we have:

Lemma 3 *Let A be initialized to the uniform superposition $\sum_g |g\rangle / \sqrt{|G|}$. Then the set of possible output states is given by the set of positive matrices with trace one contained in $R\mathcal{A}R$, where R is the reflection $|g\rangle \mapsto |g^{-1}\rangle$ and \mathcal{A} is the C^* -algebra generated by the matrices V_g .*

Proof: Let

$$|\psi\rangle := \sum_g c_g |g\rangle$$

be an arbitrary input state. Due to Eq. (4) the output state σ on A is given by

$$\left(\frac{1}{|G|} \sum_{gh} \bar{c}_g c_h \langle g | V_{m^{-1}r} | h \rangle \right)_{m,r \in G}.$$

The inner product is 1 for all $mg = rh$ and 0 otherwise. Elementary calculations show

$$\sigma = R \left(\frac{1}{|G|} \left(\sum_g \bar{c}_g V_g \right) \left(\sum_h c_h V_h^\dagger \right) \right) R.$$

Thus, σ is, up to the inversion R , an element of \mathcal{A} (which is isomorphic to the group algebra CG [32]). Let σ be an arbitrary positive element of $R\mathcal{A}R$ with trace one. Since $R\mathcal{A}R$ is closed with respect to square roots we can find an $a \in R\mathcal{A}R$ such that $a^\dagger a = \sigma$. We can write a as $a = R \sum_g c_g V_g / \sqrt{|G|}$ and hence we obtain $\rho = R(\sum_g c_g V_g)^\dagger (\sum_g c_g V_g) R / |G|$. Due to $\sum_g |c_g|^2 = \text{tr}(\rho) = 1$ the coefficient vector $(c_g)_{g \in G}$ is a unit vector and represents therefore a possible input state. \square

Using the explicit characterization of output states for the case that A is initialized to a uniform superposition we can calculate the backward channel capacity (even without restricting to uniform initializations):

Theorem 4 *The backward information capacity satisfies*

$$C(A \leftarrow B) = \log N ,$$

where N is the sum of the degrees of all inequivalent irreducible representations of G .

Proof: Let us first assume that A is initialized to $\sum_g |g\rangle/\sqrt{|G|}$. The algebra \mathcal{A} generated by the representation matrices V_g is given by [32, 33]

$$\mathcal{A} = F^\dagger \left(\bigoplus_r \mathbf{1}_r \otimes \mathcal{M}_r \right) F . \quad (10)$$

The sum runs over all inequivalent representations r . Their degree is denoted by d_r and $\mathbf{1}_r$ denotes the identity of dimension d_r . F is the generalized Fourier transform that achieves block diagonalization of \mathcal{A} . The multiplicities are irrelevant for the channel capacity. Therefore we may identify the set of possible output states with the density matrices in

$$\bigoplus_r \mathcal{M}_r ,$$

acting on a Hilbert space of dimension $N = \sum_r d_r$. This shows that the capacity is at most $\log N$. On the other hand, we can obtain every output state that is given by one entry 1 on one of the N diagonal positions. Hence, the capacity is $\log N$.

Now we drop the assumption that A is initially in a uniform superposition. Instead, we assume

$$|\phi\rangle := \sum_g \sqrt{p_g} |g\rangle$$

to be the state of A before U is applied. With respect to the original basis $|g\rangle$, this changes the output according to the map

$$F_p : \sigma \mapsto D\sigma D . \quad (11)$$

where D is the diagonal operator with entries $\sqrt{p_g}/\sqrt{|G|}$. The domain of F_p is the smallest C^* -algebra containing every possible output state, i.e., $R\mathcal{A}R$. Note that this specification of the domain makes F_p trace-preserving because all elements of $R\mathcal{A}R$ are constant along the diagonal. This implies that the diagonal of $D\sigma D$ is given by the values p_g if σ has the diagonal entries $1/|G|$. Hence we have shown that the deformation is a quantum channel. Thus, the deformed outputs cannot provide more information about the input than the undeformed outputs by monotonicity of Holevo information [34]. \square

The number N coincides with $|G|$ if and only if G is abelian. This is because the number of inequivalent representations coincides with the number of conjugacy classes [33] which is $|G|$ for abelian groups. For non-abelian groups, we have necessarily representations of degree greater than 1 and hence multiplicities greater than 1. This leads immediately to the following observation:

Corollary: *If A controls the regular representation matrices of G on B then*

$$C(A \rightarrow B) = C(A \leftarrow B)$$

if and only if G is abelian.

Even though it is not known what the smallest possible ratio would be for $C(A \leftarrow B)/C(A \rightarrow B)$ representation theory provides a lower bound for the case of regular representations:

Lemma 4 *Let $g \mapsto V_g$ be the regular representation of a finite group. Then the ratio between backward and forward capacity satisfies*

$$\frac{C(A \leftarrow B)}{C(A \rightarrow B)} \geq \frac{1}{2}.$$

Proof: We have

$$N^2 = \left(\sum_r d_r \right)^2 \geq \sum_r d_r^2 = |G|.$$

Hence $\log N \geq (\log G)/2$. \square .

The lower bound $1/2$ is asymptotically reached by $G = S_n$, i.e., the symmetric group on n points if n tends to infinity. With $|G| = n!$ we obtain an estimation of $C(A \rightarrow B)$ from Stirling's formula stating that $n!$ increases with $\sqrt{2\pi n}(n/e)^n(1 + O(1/n))$. If we measure information in terms of natural units, we obtain hence

$$\lim_{n \rightarrow \infty} \left(C(A \leftarrow B) - (\ln(\sqrt{2\pi n}) + n \ln n - n) \right) = 0.$$

An upper bound on $C(A \leftarrow B)$ can be derived from

$$\sum_r d_r \leq p_n m_n,$$

where p_n is the number of inequivalent representations of S_n and m_n the degree of the largest representation, i.e., $m_n := \max_r \{d_r\}$. An upper bound on m_n is given by [35]:

$$m_n \leq (2\pi n)^{1/4} \left(\frac{n}{e} \right)^{n/2}.$$

For p_n we have [36]

$$p_n \leq c \exp \left(\pi \sqrt{\frac{2}{3}n} \right),$$

with an appropriate constant c . With $\log N \leq \log p_n + \log m_n$ the only asymptotically relevant term is $(n \ln n)/2$. For the asymptotics of $\log |G|$, the dominating term is $n \log n$. Hence S_n reaches asymptotically the minimal possible quotient $1/2$. Figure 1 shows that the values get already quite close to $1/2$ for $n = 32$.

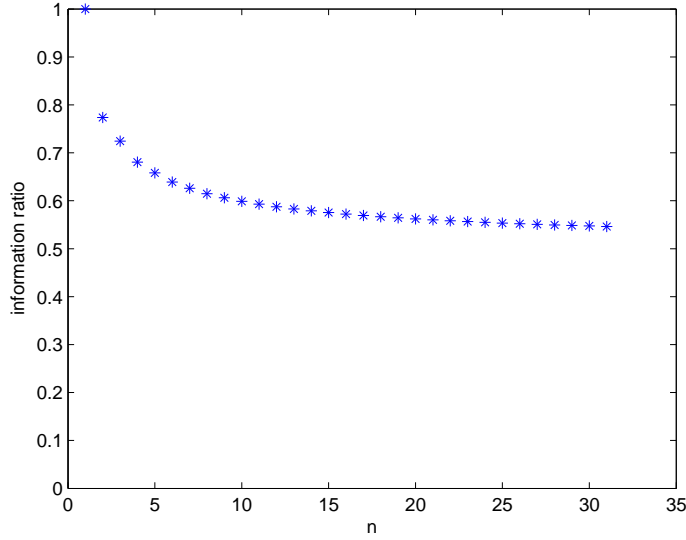


Figure 1: Ratio $C(A \leftarrow B)/C(A \rightarrow B)$ for the regular representation of S_n for $n = 2, \dots, 32$. Note that S_2 leads to the controlled-not gate.

6 The symmetric group S_3

In this section we want to provide a bit more intuition about the general results of the previous sections. The smallest non-abelian group is S_3 , the set of permutations of 3 elements (which is isomorphic to the dihedral group D_3). Since $|S_3| = 3! = 6$ the unitary operation defined by the regular representation according to Eq. (9) leads to the bipartite system $\mathbb{C}^6 \otimes \mathbb{C}^6$. We choose the generating transpositions $a := (1\ 2)$ and $b := (2\ 3)$. In every component \mathbb{C}^6 the basis vectors are labelled by g where we have chosen the following order of the elements

$$[g_1, \dots, g_6] := [(), (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)].$$

The group S_3 has three inequivalent representations of dimensions $d_1 = 1$, $d_2 = 1$, and $d_3 = 2$. Up to unitary equivalence, they are given as follows.

$$\tau_1(g) := (1) \quad \text{and} \quad \tau_2(g) := (\text{sgn}(g))$$

with the signum function sgn . Here (\cdot) denotes a (1×1) -matrix. The two-dimensional representation τ_3 is given by

$$\tau_3(a) := \begin{pmatrix} 0 & \omega_3^2 \\ \omega_3 & 0 \end{pmatrix} \quad \text{and} \quad \tau_3(b) := \begin{pmatrix} 0 & \omega_3 \\ \omega_3^2 & 0 \end{pmatrix}$$

where ω_3 is a third complex root of unity.

τ_1 and τ_2 occur with multiplicity 1 and τ_3 with multiplicity 2. If system A is in a uniform superposition the set of possible output states σ is unitarily equivalent to the set

$$(p_1) \oplus (p_2) \oplus \frac{1}{2}p_3(\sigma_2 \oplus \sigma_2), \quad (12)$$

where the non-negative scalars p_1, p_2, p_3 with $\sum_j p_j = 1$ define a probability distribution and σ_2 is an arbitrary two-dimensional density matrix.

The isomorphism between the possible output states with respect to the original basis $|g\rangle$ is described by the Fourier matrix F that decomposes the regular representation

$$\tau_{\text{reg}}(g) = \sum_h |gh\rangle\langle h|$$

into the direct sum

$$F^\dagger \tau_{\text{reg}}(g) F = \tau_1(g) \oplus \tau_2(g) \oplus \tau_3(g) \oplus \tau_3(g).$$

For our example we find the unitary

$$F = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & \sqrt{2} & 0 & 0 & \sqrt{2} \\ 1 & -1 & 0 & \sqrt{2}\omega_3 & \sqrt{2}\omega_3^2 & 0 \\ 1 & -1 & 0 & \sqrt{2} & \sqrt{2} & 0 \\ 1 & 1 & \sqrt{2}\omega_3 & 0 & 0 & \sqrt{2}\omega_3^2 \\ 1 & 1 & \sqrt{2}\omega_3^2 & 0 & 0 & \sqrt{2}\omega_3 \\ 1 & -1 & 0 & \sqrt{2}\omega_3^2 & \sqrt{2}\omega_3 & 0 \end{pmatrix}.$$

We choose the following 4 input states:

$$\begin{aligned} |\phi_1\rangle &:= \frac{1}{\sqrt{6}}(1, 1, 1, 1, 1, 1)^T, & |\phi_2\rangle &:= \frac{1}{\sqrt{6}}(1, -1, -1, 1, 1, -1)^T \\ |\phi_3\rangle &:= \frac{1}{\sqrt{3}}(1, 0, 0, \omega_3^2, \omega_3, 0)^T, & |\phi_4\rangle &:= \frac{1}{\sqrt{3}}(0, 1, \omega_3, 0, 0, \omega_3^2)^T. \end{aligned}$$

They generate the output states

$$\begin{aligned} \sigma_1 &:= \text{diag}(1, 0, 0, 0, 0, 0), & \sigma_2 &:= \text{diag}(0, 1, 0, 0, 0, 0) \\ \sigma_3 &:= \frac{1}{2}\text{diag}(0, 0, 1, 0, 1, 0), & \sigma_4 &:= \frac{1}{2}\text{diag}(0, 0, 0, 1, 0, 1). \end{aligned} \quad (13)$$

We obtain $C(A \rightarrow B) = \log 6$ and $C(A \leftarrow B) = \log 4$.

The following example shows that the statements of Section 5 do not apply to non-regular representations. If we choose the usual permutation representation of S_3 we obtain a unitary transformation on $\mathbb{C}^6 \otimes \mathbb{C}^3$, where the action of S_3 on \mathbb{C}^3 is defined by

$$\tau(a) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \tau(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

We have $C(A \rightarrow B) = \log 3$ because we can clearly obtain 3 mutually orthogonal states on B by choosing any canonical basis vector of \mathbb{C}^3 as initial state. Even though S_3 is non-abelian we also have $C(A \leftarrow B) = \log 3$. Using the three input vectors

$$|\Phi_1\rangle := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad |\Phi_2\rangle := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega_3 \\ \omega_3^2 \end{pmatrix} \quad |\Phi_3\rangle := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega_3^2 \\ \omega_3 \end{pmatrix}$$

the output density operators read $\sigma_1, \sigma_3, \sigma_4$ as defined in Eq. (13).

7 What's the message?

We have shown that a unitary operation on a bipartite finite-dimensional system A, B can only enable information transmission from A to B whenever there is also information transmission possible from B to A . However, for arbitrarily high dimensions the difference between backward channel capacity and forward capacity can be arbitrarily large. To show this we have constructed bipartite unitary operations of the following type: mutually orthogonal states on A control the implementation of unitary operations on B taken from a finite group. Then the backaction becomes smaller the less abelian the group is.

To link our results to the philosophical questions raised in the introduction we assume that A is a toy model of a quantum controller. We assume that the interaction between controller A and the system to be controlled (denoted by B) implements

$$U = \sum_j P_j \otimes V_j,$$

(where P_j may also be degenerate projections) after influencing the system during some fixed time interval. Let $|\phi\rangle$ be the state of system A . If $|\phi\rangle \in P_j \mathcal{H}_A$ for some j the system A is insensitive. However, if the controller state is switched from one subspace $P_j \mathcal{H}_A$ to another $P_i \mathcal{H}_A$ there must be a moment where it is a superposition. During the switching process, A is necessarily influenced by B and this paper has tried to clarify to what extent this influence depends on the state of B . For small dimensions, this back action cannot be arbitrarily small. At first glance, dimension dependent bounds seem to be of minor interest if one thinks of the quantum controller as a large quantum system. However, our bound in Section 4 depends on the *minimum* of the dimensions of controller and system. To find tight lower bounds on the backward capacity in terms of the forward capacity has to be left to the future.

Acknowledgments

The authors would like to thank Martin Rötteler and Pawel Wocjan for helpful discussions and Aram Harrow for useful comments. TD was supported under ARO/NSA quantum algorithms grant number W911NSF-06-1-0379.

References

- [1] R. Omnès. *The interpretation of quantum mechanics*. Princeton Series in Physics. Princeton University Press, 1994.
- [2] J. Jauch. *Foundations of quantum mechanics*. Addison-Wesley, Reading, Mass., 1968.
- [3] C. Fuchs. Information Gain vs. State Disturbance in Quantum Theory. arXiv:quant-ph/9611010, 1996.

- [4] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [5] S. Lloyd. Quantum controllers for quantum systems. arXiv:quant-ph/9703042.
- [6] N. Khaneja, S. Glaser, and R. Brockett. Sub-Riemannian geometry and time optimal control of three spin systems: Quantum gates and coherence transfer. *Phys. Rev. A*, 71:039906, 2005.
- [7] D. Janzing, F. Armknecht, R. Zeier, and T. Beth. Quantum control without access to the controlling interaction. *Phys. Rev. A*, 65:022104, 2002.
- [8] S. Lloyd, A. Landahl, and E. Slotine. Universal quantum interfaces. *Phys. Rev. A*, 69:0512305, 2004.
- [9] K. Hepp. Quantum theory of measurement and macroscopic observables. *Helv. Phys. Acta*, 49:237–248, 1972.
- [10] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. Roy. Soc. London A*, 454:339–354, 1998.
- [11] P. Wocjan and S. Zhang. Several natural BQP-complete problems. arXiv:quant-ph/0606179.
- [12] D. Janzing and B. Steudel. Quantum broadcasting problem in classical low power signal processing. *Phys. Rev. A*, 75, 2007.
- [13] D. Janzing and T. Beth. Synchronizing quantum clocks with classical one-way communication: Bounds on the generated entropy. arXiv:quant-ph/0306023v1.
- [14] D. Janzing and T. Beth. Are there quantum bounds on the recyclability of clock signals in low power computers? In *Proceedings of the DFG-Kolloquium VIVA*, Chemnitz, 2002. arXiv:quant-ph/0202059.
- [15] D. Janzing and T. Beth. Quasi-order of clocks and their synchronism and quantum bounds for copying timing information. *IEEE Trans. Inform. Theor.*, 49(1):230–240, 2003.
- [16] J. Cortese. Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels. *Phys. Rev.*, A(69):022302, 2004.
- [17] A. Holevo. The capacity of quantum channel with general signal states. *IEEE Trans. Inf. Th.*, 44:269–273, 1998.
- [18] C. Bennett, A. Harrow, D. Leung, and J. Smolin. On the capacities of bipartite hamiltonians and unitary gates. arXiv:quant-ph/0205057v4.
- [19] A. Harrow and P. Shor. Time reversal and exchange symmetries of unitary gate capacities. arXiv:quant-ph/0511219.
- [20] N. Linden, J. Smolin, and A. Winter. The entangling and disentangling power of unitary transformations are unequal. arXiv:quant-ph/0511217.
- [21] A. Chefles. Entangling capacity and distinguishability of two-qubit unitary operators. *Phys. Rev.*, A(72):042332, 2005.
- [22] X. Wang and P. Zanardi. Quantum entanglement of unitary operators on bi-partite systems. *Phys. Rev.*, A(66), 044303 2002.

- [23] L. Faoro, P. Zanardi, C. Zalka. On the entangling power of quantum evolutions. arXiv:quant-ph/0005031.
- [24] B. Kraus, M. Lewenstein I. Cirac, W. Dür. Entangling operations and their implementation using a small amount of entanglement. *Phys. Rev. Lett.*, 86:544, 2001.
- [25] I. Cirac, W. Dür, B. Kraus, and M. Lewenstein. Entangling operations and their implementation using a small amount of entanglement. *Phys. Rev. Lett.*, 86:544, 2001.
- [26] W. Dür, G. Vidal, I. Cirac, N. Linden, and S. Popescu. Entanglement capabilities of non-local Hamiltonians. *Phys. Rev. Lett.*, 87:137901, 2001.
- [27] B. Kraus and I. Cirac. Optimal creation of entanglement using a two-qubit gate. arXiv:0011050.
- [28] M. Leifer, L. Henderson, and N. Linden. Optimal entanglement generation from quantum operations. *Phys. Rev. A*, 67:012306, 2003.
- [29] D. Berry and B. Sanders. Relation between classical communication capacity and entanglement capability for two-qubit unitary operations. *Phys. Rev.*, A(68):032312, 2003.
- [30] G. Murphy. *C*-algebras and operator theory*. Academic Press, Boston, 1990.
- [31] N. Khaneja, R. Brockett, and S. Glaser. Time optimal control in spin systems. *Phys. Rev. A*, 63(3):032308, 2001.
- [32] M. Clausen and U. Baum. *Fast Fourier transforms*. Bibliographisches Institut, Mannheim, 1993.
- [33] J.-P. Serre. *Linear representations of finite groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1977.
- [34] D. Petz. Monotonicity of quantum relative entropy revisited. *Rev. Math. Phys.*, 15:79–91, 2003.
- [35] J. McKay. The largest degree of irreducible characters of the symmetric group. *Mathematics of Computation*, 30(135):624–631, 1976.
- [36] G. Andrews. *The theory of partitions*. Cambridge University Press, 1984.